IKEv2 Notification Status Types for IPv4/IPv6 Coexistence
draft-ietf-ipsecme-ipv6-ipv4-codes-06

Abstract

   This document specifies new IKEv2 notification status types to better
   manage IPv4 and IPv6 co-existence by allowing the responder to signal
   to the initiator which address families are allowed.

   This document updates RFC7296.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   As described in [RFC7849], if the subscription data or network
   configuration allows only one IP address family (IPv4 or IPv6), the
   cellular host must not request a second PDP-Context (Section 3.2 of
   [RFC6459]) to the same Access Point Name (APN) for the other IP
   address family (AF). The Third Generation Partnership Project (3GPP)
   network informs the cellular host about allowed Packet Data Protocol
   (PDP) types by means of Session Management (SM) cause codes. In
   particular, the following cause codes can be returned:

   o cause #50 "PDP type IPv4 only allowed": This cause code is used by
      the network to indicate that only PDP type IPv4 is allowed for the
      requested Public Data Network (PDN) connectivity.

   o cause #51 "PDP type IPv6 only allowed": This cause code is used by
      the network to indicate that only PDP type IPv6 is allowed for the
      requested PDN connectivity.

   o cause #52 "single address bearers only allowed": This cause code
      is used by the network to indicate that the requested PDN
      connectivity is accepted with the restriction that only single IP
      version bearers are allowed.

   If the requested IPv4v6 PDP-Context is not supported by the network
   but IPv4 and IPv6 PDP types are allowed, then the cellular host will
   be configured with an IPv4 address or an IPv6 prefix by the network.
   It must initiate another PDP-Context activation of the other address
   family in addition to the one already activated for a given APN. The
   purpose of initiating a second PDP-Context is to achieve dual-stack

connectivity (that is, IPv4 and IPv6 connectivity) by means of two PDP-Contexts.

When the User Equipment (UE) attaches to the 3GPP network using a non-3GPP access network (e.g., Wireless Local Area Network (WLAN)), there are no equivalent Internet Key Exchange Protocol Version 2 (IKEv2) capabilities [RFC7296] notification codes for the 3GPP network to inform the UE why an IP address family is not assigned or whether that UE should retry with another address family.

This document fills that void by introducing new IKEv2 notification status types for the sake of deterministic UE behaviors (Section 4).

These notification status types are not specific to 3GPP architectures, but can be used in other deployment contexts. Cellular networks are provided as an illustration example.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

This document makes use of the terms defined in [RFC7296]. In particular, readers should be familiar with "initiator" and "responder" terms used in that document.

3. Why Not INTERNAL_ADDRESS_FAILURE?

The following address assignment failures may be encountered when an initiator requests assignment of IP addresses/prefixes:

o An initiator asks for IPvx, but IPvx address assignment is not supported by the responder.

o An initiator requests both IPv4 and IPv6 addresses, but only IPv4 address assignment is supported by the responder.

o An initiator requests both IPv4 and IPv6 addresses, but only IPv6 prefix assignment is supported by the responder.

o An initiator asks for both IPv4 and IPv6 addresses, but only one address family can be assigned by the responder for policy reasons.

Section 3.15.4 of [RFC7296] defines a generic notification error type
(INTERNAL_ADDRESS_FAILURE) that is related to a failure to handle an
address assignment request. The responder sends
INTERNAL_ADDRESS_FAILURE only if no addresses can be assigned. This
behavior does not explicitly allow an initiator to determine why a
given address family is not assigned, nor whether it should try using
another address family. INTERNAL_ADDRESS_FAILURE is a catch-all
error type when an address-related issue is encountered by an IKEv2
responder.

INTERNAL_ADDRESS_FAILURE does not provide sufficient hints to the
IKEv2 initiator to adjust its behavior.

4. IP6_ALLOWED and IP4_ALLOWED Status Types

IP6_ALLOWED and IP4_ALLOWED notification status types (see Section 7)
are defined to inform the initiator about the responder's address
family assignment support capabilities, and to report to the
initiator the reason why an address assignment failed. These
notification status types are used by the initiator to adjust its
behavior accordingly (Section 5).

No data is associated with these notifications.

5. An Update to RFC7296

If the initiator is dual-stack (i.e., supports both IPv4 and IPv6),
it MUST include both address families configuration attributes in its
configuration request (absent explicit policy/configuration
otherwise). More details about IPv4 and IPv6 configuration
attributes are provided in Section 3.15 of [RFC7296]. These
attributes are used to infer the requested/assigned AFs listed in
Table 1.

The responder MUST include IP6_ALLOWED and/or IP4_ALLOWED
notification status type in a response to an address assignment
request as indicated in Table 1.

Requested AF(s) (Initiator)	Supported AF(s) (Responder)	Assigned AF(s) (Responder)	Returned Notification Status Type(s) (Responder)
IPv4	IPv6	None	IP6_ALLOWED
IPv4	IPv4	IPv4	IP4_ALLOWED
IPv4	IPv4 and IPv6	IPv4	IP4_ALLOWED, IP6_ALLOWED
IPv6	IPv6	IPv6	IP6_ALLOWED
IPv6	IPv4	None	IP4_ALLOWED
IPv6	IPv4 and IPv6	IPv6	IP4_ALLOWED, IP6_ALLOWED
IPv4 and IPv6	IPv4	IPv4	IP4_ALLOWED
IPv4 and IPv6	IPv6	IPv6	IP6_ALLOWED
IPv4 and IPv6	IPv4 and IPv6	IPv4 and IPv6	IP4_ALLOWED, IP6_ALLOWED
IPv4 and IPv6	IPv4 or IPv6 (Policy-based)	IPv4 or IPv6	IP4_ALLOWED, IP6_ALLOWED

Table 1: Returned Notification Status Types

If the initiator only receives one single notification IP4_ALLOWED or IP6_ALLOWED from the responder, the initiator MUST NOT send a subsequent request for an alternate address family not supported by the responder.

If a dual-stack initiator requests only an IPv6 prefix (or an IPv4 address) but only receives IP4_ALLOWED (or IP6_ALLOWED) notification status type from the responder, the initiator MUST send a request for IPv4 address(es) (or IPv6 prefix(es)).

If a dual-stack initiator requests both an IPv6 prefix and an IPv4 address but receives an IPv6 prefix (or an IPv4 address) only with both IP4_ALLOWED and IP6_ALLOWED notification status types from the responder, the initiator MAY send a request for the other AF (i.e., IPv4 address (or IPv6 prefix)). In such case, the initiator MUST create a new IKE Security Association (SA) and request that another address family using the new IKE SA.

For other address-related error cases that have not been covered by the aforementioned notification status types, the responder/initiator MUST follow the procedure defined in Section 3.15.4 of [RFC7296].

6. Security Considerations

Since the IPv4/IPv6 capabilities of a node are readily determined
from the traffic it generates, this document does not introduce any
new security considerations compared to the ones described in
[RFC7296], which continue to apply.

7. IANA Considerations

This document requests IANA to update the "IKEv2 Notify Message Types
- Status Types" registry available at:
https://www.iana.org/assignments/ikev2-parameters/
ikev2-parameters.xhtml with the following status types:

```
Value              NOTIFY MESSAGES - STATUS TYPES      Reference
 TBD                      IP4_ALLOWED                [This-Document]
 TBD                      IP6_ALLOWED                [This-Document]
```

8. Acknowledgements

Many thanks to Christian Jacquenet for the review.

Thanks to Paul Wouters, Yaov Nir, Valery Smyslov, Daniel Migault,
Tero Kivinen, and Michael Richardson for the comments and review.

Thanks to Benjamin Kaduk for the AD review.

Thanks to Murray Kucherawy, Eric Vyncke, and Robert Wilton for the
IESG review.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119,
           DOI 10.17487/RFC2119, March 1997,
           <https://www.rfc-editor.org/info/rfc2119>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T.
           Kivinen, "Internet Key Exchange Protocol Version 2
           (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October
           2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
           2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
           May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

   [RFC6459] Korhonen, J., Ed., Soininen, J., Patil, B., Savolainen,
              T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation
              Partnership Project (3GPP) Evolved Packet System (EPS)",
              RFC 6459, DOI 10.17487/RFC6459, January 2012,
              <https://www.rfc-editor.org/info/rfc6459>.

   [RFC7849] Binet, D., Boucadair, M., Vizdal, A., Chen, G., Heatley,
              N., Chandler, R., Michaud, D., Lopez, D., and W. Haeffner,
              "An IPv6 Profile for 3GPP Mobile Devices", RFC 7849,
              DOI 10.17487/RFC7849, May 2016,
              <https://www.rfc-editor.org/info/rfc7849>.

Author's Address

   Mohamed Boucadair
   Orange
   Rennes 35000
   France

   Email: mohamed.boucadair@orange.com